Pending Claims

The listing of claims will replace all prior versions, and listings of claims in the application.

1. (Previously Presented) A server to perform computations to establish a secure network session, comprising of:

a system memory; and

a processing unit coupled to said system memory via a system bus, the processing unit obtains values for a modulus N, a private key d, and a cipher text C sent by a client and calculates a value for clear text M for each request for a secure network session made to the server by the client, the processing unit includes:

an execution unit, coupled to a decode unit, configured to execute arithmetic instructions to perform product and square operations, the execution unit including at least one adder and at least two multipliers configurable to perform specified multiplication operations in parallel and configurable to perform specified multiplication and addition operations in parallel;

the decode unit to receive requests for establishing a secure network session from the client, the decode unit configured to determine if a square operation or a product operation needs to be performed on an operand, the decode unit further configured to issue the arithmetic instructions to the execution unit so that the execution unit performs specified multiplication and addition operations in parallel and performs specified multiplication operations in parallel while performing either the square or product operation.

2. (Previously Presented) The server of claim 1, wherein the decode unit is configured to issue a set of instructions that causes the execution unit to perform the specified multiplication and addition operations in parallel to reduce the number of cycles required to perform the product operation.

3. (Cancelled)

4. (Previously Presented) The server of claim 3, wherein certain of the multiplication operations are performed in parallel using a multiply and shift by one instruction.

5 - 6. (Cancelled)

7. (Previously Presented) The server of claim 1, wherein the decode unit is further configured to decode an operation $M=C^d \bmod N$ by:

(a) determining the MSB position of the exponent d equal to a first logic state;

(b) issuing a first set of instructions to implement a square and a product operation after the MSB position of the exponent d equal to a first logic state is determined;

(c) determining if the next most significant bit (MSB) of exponent (d) is of the first logic state or a second logic state; and either

(d) issuing a second set of instructions to the execution unit to implement a square operation if the next MSB is of the second logic state; or

(e) issuing the first set of instructions to the execution unit if the next MSB of the exponent is of the first logic state to implement a square and a product operation; and

repeating (c) through (e) for every bit in the exponent (d) from the next MSB to the least significant bit (LSB).

8. (Previously Presented) The server of claim 7, wherein the final result of the operation $M=C^d \bmod N$ is obtained by accumulating the results of (b) through (e).

9. (Previously Presented) The server of claim 1, wherein the encryption processor is located in a server and is used to establish a secure socket layer connection between the server and a client.

10 - 11. (Cancelled)

12. (Previously Presented) The server of claim 1 wherein the product and square operations executed by the execution unit are Montgomery product and square operations.

13. (Cancelled)

14. (Previously Presented) The server of claim 1, wherein the encryption processor is configured into a web server deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

15. (Previously Presented) The server of claim 1, wherein the encryption processor is configured into a secure switch deploying Secure Socket Layer (SSL)/Transport Layer Security(TLS).

16. (Previously Presented) The server of claim 1, wherein the encryption processor is configured into an Internet load balance device with Secure Socket Layer (SSL)/Transport Layer Security(TLS) termination functionality.

17. (Previously Presented) The server of claim 1 wherein the encryption processor is configured into an Internet appliance for a Virtual Private Network.

18. (Previously Presented) The server of claim 1 wherein the encryption processor is configured into a security based router.

19. (Previously Presented) The server of claim 1 wherein the encryption processor is configured into a remote access device used for VPN applications.

20. (Previously Presented) The server of claim 1, wherein the encryption processor is configured into one or more of the following: concentrator-based security systems for

enterprise and ISPs; subscriber management systems with VPN support; firewalls with VPN support; and VPN gateways.

21. (Previously Presented) A method to establish a secure network session, comprising the steps of:

sending an encrypted message to a server using a public key;

decrypting said encrypted message by the server using a private key; and

generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and the server, wherein generation of the public key, the private key, and/or the symmetrical key further comprises computation of a modular exponentiation operation using the Montgomery method, wherein said Montgomery method further comprises:

receiving, by a decode unit, a request to perform a modular operation;

determining, by the decode unit, whether a Montgomery square operation or a Montgomery product operation is to be performed;

issuing, by the decode unit, a first instruction to perform a Montgomery square operation;

issuing, by the decode unit, a second instruction to perform a Montgomery product operation;

performing, by an execution unit, simultaneous multiplication operations in response to at least one of the first instruction and the second instruction; and

performing, by the execution unit, simultaneous multiplication and addition operations in response to at least one of the first instruction and the second instruction.

22. (Previously Presented) A method to establish a secure network session, comprising the steps of:

sending an encrypted message to a server using a public key;

decrypting said encrypted message by said server using a private key; and

generating a symmetrical key to encrypt/decrypt messages transmitted and received between a client and said server, wherein said public key, said private key, and/or said symmetrical key further comprises computation of a modular exponentiation operation using the Montgomery method, wherein said Montgomery method further comprises:

determining, by a decode unit, whether to perform a Montgomery square operation or a Montgomery product operation;

issuing, by the decode unit, a first set of instructions for an execution unit to perform the Montgomery square operation, the first set of instructions comprising;

a first instruction to perform simultaneous multiplication operations; and

a second instruction to perform simultaneous multiplication and addition operations; and

issuing, by the decode unit, a second set of instructions for an execution unit to perform the Montgomery product operation, the second set of instructions comprising:

a third instruction to perform simultaneous multiplication operations;

a fourth instruction to perform simultaneous multiplication and addition operations; and

a fifth instruction to perform simultaneous multiplication and addition operations.

23. (Previously Presented) The server of claim 1, wherein the at least one adder and at least two multipliers perform the specified multiplication operations in parallel in a first clock cycle.

24. (Previously Presented) The server of claim 23, wherein the at least one adder and at least two multipliers perform the specified multiplication and addition operations in parallel in a second clock cycle that immediately follows the first clock cycle.

25. (Previously Presented) The server of claim 1, wherein the at least one adder and at least two multipliers perform either specified multiplication operations in parallel or perform specified multiplication and addition operations in parallel in accordance with the issued instructions.

26. (Previously Presented) The server of claim 1, wherein the decode unit determines whether a square operation or a product operation needs to be performed on an operand for a modular operation.

27. (Previously Presented) The server of claim 26, wherein the at least one adder and at least two multipliers perform either specified multiplication operations in parallel or perform specified multiplication and addition operations in parallel in accordance with the determination of whether a square operation or a product operation needs to be performed.

28. (Previously Presented) The server of claim 1, wherein the arithmetic instructions comprise a set of micro instructions.

29. (Previously Presented) The server of claim 1, wherein the arithmetic instructions comprise plurality of types of add-subtract instructions and a plurality of types of multiply instructions.

30. (Previously Presented) The server of claim 1, wherein the value for clear text M is calculated using the Montgomery method.